Vaatame ElGamali signatuuriskeemi rühmas $\mathbb{Z}_p^*$, kus p ja $q = \frac{p-1}{2}$ on algarvud. Näita, et kui ründaja võib valida $\mathbb{Z}_p^*$ moodustaja g, siis suudab ta ka signatuure võltsida.

Vihje: ründaja valib mingi $t \in \mathbb{Z}_{p-1}^*$ ja võtab $g = q^t \bmod p$ (kui q ei ole $\mathbb{Z}_p^*$ moodustaja, siis rünne ei õnnestu). Signatuuri (τ, s) genereerides võtab ta τ võrdseks q-ga.

Olgu E mingi plokkšifri šifreerimisfunktsioon, s.t. $E_a(b)$ šifreerib avateksti b võtmega a. Olgu nii võtmete kui ka avatekstide pikkus n. Vaatame kompressioonifunktsiooni $h(x_1, x_2) = E_{x_1 \oplus x_2}(x_2) \oplus x_1 \oplus x_2$, kus x_1 ja x_2 on bitijadad pikkusega n. Näita, kuidas leida funktsiooni h kollisioone, kui me võime välja kutsuda E-d ja dešifreerimisfunktsiooni D meie valitud argumentidel.

Kasutades eelmise ülesande tähistusi, olgu nüüd $H(x_1, x_2) = E_{x_1}(x_2) \oplus E_{x_2}(x_1) \oplus x_2$. Kasutades seda kompressioonifunktsiooni, defineerime räsifunktsiooni $H^* : (\{0,1\}^n)^* \longrightarrow \{0,1\}^n$ järgmiselt:

$$H^*(x_1, \ldots, x_m) = H(H(\cdots H(H(z, x_1), x_2) \cdots), x_{m-1}), x_m)$$

kus z on 0-dest koosnev bitijada pikkusega n. Näita, et H^* ei ole kollisioonikindel.

Vihje: Millega võrdub $H(x, x)$? Kuidas seda kollisiooni konstrueerimise juures ära kasutada?

Olgu G mingi raske diskreetse logaritmiga rühm, $m = |G|$, olgu $g \in G$. Olgu $h = g^a$ mingi $a \in \mathbb{Z}_m$ jaoks. Kui Alice teab a-d, siis kuidas saab ta Bobile nullteadmusega tõestada, et $h \in \langle g \rangle$?

Olgu $n = pq$ RSA moodul, olgu $s \in \mathbb{Z}_n^*$ ja $v = s^2 \bmod n$. Kui Alice teab s-i, siis kuidas saab ta Bobile nullteadmusega tõestada, et v on ruutjääk *modulo* n?

Olgu meil antud rühm G, kus Diffie-Hellmani ülesanne on raske, olgu $|G| = m$ ja olgu g selle rühma mingi moodustaja. Olgu meil ka teada Alice'i ElGamali krüptosüsteemi avalik võti $h = g^a$ (a ei ole teada). Olgu $m \in G$. Me moodustame m-st Alice'i avaliku võtmega kaks erinevat krüptoteksti (g^r, mh^r) ja $(g^{r'}, mh^{r'})$ ning avalikustame need. Kuidas me saame Bob'ile tõestada, et need kaks krüptoteksti vastavad tõepoolest samale avatekstile, avalikustamata seejuures teadet m?

Kuidas saaks Alice sama väidet tõestada?

Bitikinnistusskeemi võib luua järgmisel viisil. Olgu $n = pq$ RSA moodul, mille on konstrueerinud usaldatud kolmas osapool (s.t. tegurid p ja q pole teada ei kinnistajale ega ka kontrollijale). Kinnistamaks bitti 0 valib kinnistaja mingi paarisarvu x hulgast $\{0, \ldots, n-1\}$; kinnistamaks bitti 1 valib ta mingi paaritu arvu x sellest hulgast. Biti b kinnistuseks on arv $y = x^2 \bmod n$. Avamiseks saadab kinnistaja kontrollijale biti b ja arvu y. Kontrollija kontrollib, et $b = x \bmod 2$ ja $y = x^2 \bmod n$. Miks on see skeem ebaturvaline?

(Biti)kinnistus, mille turvalisus põhineb diskreetse logaritmi raskusel?

Olgu G rühm, g moodustaja, $h \in G$. Kinnistamaks teadet $m \in \{0, \ldots, |G| - 1\}$ valime mingi $r \in \{0, \ldots, |G| - 1\}$ ja arvutame

$$C(m; r) = g^m h^r$$

Avamiseks saadame kontrollijale m ja r.

Peitmine? Sidumine? Mis eeldustel? Kas absoluutne või arvutuslik?

Vaatame järgmist identifitseerimisskeemi. Alice genereerib RSA mooduli $n = pq$. Alice'i avalik võti on n, salajane võti on (p, q). Kui Alice soovib end Bobile identifitseerida, siis genereerib Bob juhusliku ruutjäägi $x \in \mathbb{Z}_n$ ja saadab selle Alice'ile. Alice leiab sellise $y \in \mathbb{Z}_n$, et $y^2 \equiv x \pmod{n}$, ja saadab selle tagasi. Bob kontrollib, et $y^2 \equiv x \pmod{n}$ ja loeb Alice'i identifitseerituks, kui see tõepoolest nii on. Miks on see skeem ebaturvaline?

Tuntud krüptograaf hr. Kass otsustas rakendada RSA krüptosüsteemil põhinevat identifitseerimisskeemi. Mooduliks valitakse $n = pq$, Alice'ile antakse salajane astendaja d ja Bobile avalik astendaja e. Soovides end autentida, esitab Alice Bobile paari (x, x^d) ning Bob aktsepteerib Alice'i isiku, kui $(x^d)^e \equiv x \pmod{n}$. Hinda selle süsteemi turvalisust, kui

- Alice võib ise valida suuruse x;
- Bob genereerib juhusliku suuruse x ja saadab selle Alice'ile;
- sama võtmepaari kasutatakse mitme seansi jooksul ja esimesel seansil võetakse $x = 2$, teisel $x = 3$, kolmandal $x = 4$, jne.

OCSP-protokolli kasutades peab CA iga vastuse eraldi signeerima. Signeerimine on kallis operatsioon. Kas saaks ka kuidagi harvemini signeerida?

Kas CA peab OCSP-päringutele tingimata ise vastama, või oleks võimalik see vastamine *outsource*'ida?

Vihje: Räsipuud.